PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-251660

(43)Date of publication of application : 27.09.1996

(51)Int.Cl. H04Q 7/38
G06F 1/00
G06F 12/14

(21)Application number : 07-052454

(22)Date of filing : 13.03.1995

(71)Applicant : NEC CORP

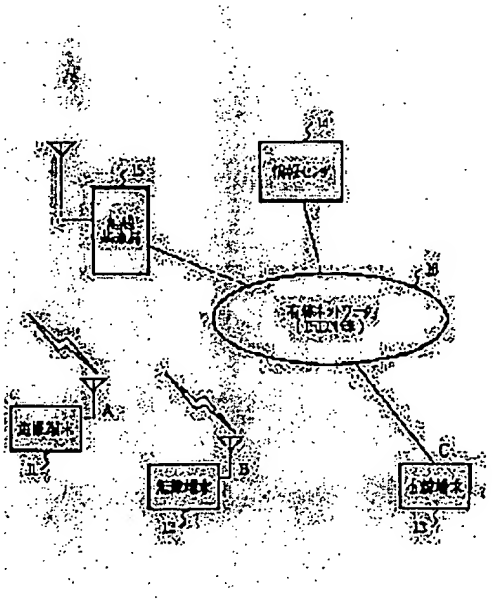
(72)Inventor : ARIGA KENICHI

(54) SUBSYSTEM FOR PREVENTING ILLICIT USE OF RADIO PORTABLE TERMINAL IN RADIO PORTBLE TERMINAL SYSTEM

(57)Abstract:

PURPOSE: To disable the use of a stolen portable terminal by outputting a system lock request from a network to the terminal based upon information from an owner of the terminal and allowing the terminal to delete its all internal data.

CONSTITUTION: An owner of a stolen radio portable terminal 11 transmits information to which the terminal ID of the terminal 11 to an information center 14 through another radio portable terminal 12 or a wired terminal 13. The center 14 transmits an ID check request command to which the terminal ID of the terminal 11 is added through a radio base station 15. When a respose is returned from the terminal 11, the center 14 transmits a system lock command to the terminal 11. Thereby the terminal 11 erases all the contents of an owner's personal data storage RAM backed up by a battery and then returns a system lock completion response to the center 14. The center 14 returns system lock completion information to the owner of the terminal 11.



LEGAL STATUS

[Date of request for examination] 13.03.1995

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 2661582

[Date of registration] 13.06.1997

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the prevention approach through the network to the unauthorized use in a wireless personal digital assistant.
[0002]
[Description of the Prior Art] Although a personal digital assistant is spreading through a world in recent years, about security reservation of a personal digital assistant, it is in a development way phase still more.
[0003] In order to lose in the conventional personal digital assistant or to secure the security at the time of suiting a theft, there is also a thing which sets up a password and is made to input at the time of starting.
[0004] Moreover, if nonvolatile storages, such as a dismountable IC card, are formed in a personal computer and the card is not mounted in it, when making it the computer itself not start, the approach of maintaining security will have indicated JP,5-94225,A.
[0005] Moreover, JP,5-145483,A displayed the owner name at the time of starting, and unless the code called a security code is inputted, it has indicated the wireless terminal with a means to forbid registration modification of an owner name.
[0006]
[Problem(s) to be Solved by the Invention] If there is no password function about a wireless personal digital assistant loss or when a theft is carried out, a third person acquires the terminal and it is used unjustly, reference of in-house datas, such as access to a wireless network and an address book, is freely possible. Moreover, even if there is a password function, an unauthorized use cannot be prevented if a password is decoded with a certain means.
[0007] The purpose of this invention is shown in preventing that a theft and the lost wireless personal digital assistant are used improperly by the third person, and aiming at improvement in security.
[0008]
[Means for Solving the Problem] This invention prevents unjust access to a network, and reference of an in-house data by making into a lock condition (unusable condition) loss or the wireless personal digital assistant by which the theft was carried out. For this reason, in the wireless personal digital assistant unauthorized use prevention approach of this invention, a means to notify that to a personal digital assistant through a wireless network from an owner before using improperly the wireless personal digital assistant acquired by the third person has attained the above-mentioned purpose by changing a personal digital assistant into a lock condition.
[0009]
[Function] If having suited the theft in the information centre is notified, after looking for a theft terminal from an information centre and checking a partner, a system lock will be carried out by transmitting the demand which eliminates internal data to a personal digital assistant. The unauthorized use of a personal digital assistant in which the theft was carried out by this can be prevented.
[0010]
[Example] Hereafter, the example of this invention is explained with reference to a drawing.
[0011] As for drawing 1 , the wireless personal digital assistant unauthorized use prevention subsystem of this invention is held. It is the structure-of-a-system Fig. of the wireless personal digital assistant system to explain, and drawing 2 is the block diagram of the wireless personal digital assistant in this system, and drawing 3 is drawing showing the sequence of the communication link with a wireless personal digital assistant and an information centre.
[0012] The hardware configuration of a wireless personal digital assistant is first explained using the block diagram of drawing 2 R> 2.
[0013] The wireless personal digital assistant consists of an input device 26 for inputting the indicator 25 for displaying RAM23 for data accumulation and information that are recording is carried out in personal data, such as ROM24 in which CPU21 which controls the whole system, the control program, etc. are accumulated, RAM22 for work pieces which a control program uses, an address book, and a schedule, and actuation, and data, and a wireless module 27 which performs control of wireless.
[0014] The data inputted with the input device 26 are stored in RAM23 for data accumulation.
[0015] Generally, since RAM23 for data accumulation is backed up by the cell, even if it drops a power source, it is not eliminated. In transmitting data on radio, it carries out by sending data to the wireless module 27 through a system bus from RAM 22 and 23 and ROM24.

[0016] Next, this structure of a system is explained using drawing 1 . Wireless personal digital assistant A (11) and B (12) are registered into the information centre 14. Moreover, the cable terminal C (13) is a terminal accessible to an information centre 14. The base transceiver station 15 and the information centre 14 are connected in the network 16 of a cable.

[0017] Now, a certain man owns wireless personal digital assistant A (11), and it is assumed that the theft was suited. The owner of wireless personal digital assistant A (11) accesses an information centre 14 through the terminal C (13) of wireless personal digital assistant [of other men] B (12), or a cable, in order to notify that there was a theft to an information centre 14. The case where it accesses at the cable terminal C (13) is explained using the notice sequence diagram of drawing 3 .

[0018] If the connection request which added ID, the telephone number, and a password from the cable terminal C (13) is transmitted and an information centre 14 receives, the completion response of connection will be returned (301 in drawing).

[0019] The notice of a theft which added the terminal ID of wireless personal digital assistant A (11) to the information centre 14 after the completion of connection is transmitted to an information centre 14 (302 in drawing). In the information centre 14 which received the notice of a theft, after returning a command check response to the cable terminal C (13), in order to check whether a theft terminal is in the condition (receptacle waiting state) which can be communicated through a base transceiver station 15, ID acknowledge request command which added ID of a theft terminal is transmitted (303 in drawing). If theft terminal A (11) is in the condition which can be communicated, the notice response of ID will be returned.

[0020] In the information centre 14 which checked the notice response of ID, since theft terminal A (11) was specified, a system-lock demand command is transmitted (304 in drawing). In theft terminal A (11) which received this command, after eliminating the contents of RAM23 for data accumulation, a system-lock completion response is transmitted to an information centre 14.

[0021] In the information centre 14 which checked the system lock of a terminal, it notifies that the terminal changed that into the lock condition by the notice of system-lock completion at the cable terminal C (13) (305 in drawing). Here, since the in-house data of theft terminal A (11) was eliminated, the security of a terminal will be maintained.

[0022]

[Effect of the Invention] After losing a personal digital assistant or suiting a theft, it becomes impossible for a third person to refer to in-house datas, such as access to a wireless network, and an address book, in order that the wireless personal digital assistant unauthorized use prevention subsystem of this invention may change a terminal into a lock condition by sending a command through a wireless network from an owner before the wireless personal digital assistant acquired by the third person is used improperly as explained above. For this reason, the security of a terminal is maintained.